Política de Ciberseguridad Corporativa

---

1. Objetivo

Proteger los sistemas, datos, propiedad intelectual y servicios digitales de SISTECOO, S.A. frente a ciberamenazas, asegurando un entorno seguro que permita la innovación y continuidad del negocio.

2. Ámbito de Aplicación

Aplica a:

- Todos los empleados, desarrolladores, equipos de soporte técnico, contratistas y terceros con acceso a sistemas y datos.
- Infraestructura tecnológica interna y en la nube (SaaS, IaaS, PaaS).

3. Principios Generales

- Seguridad desde el diseño (Security by Design).
- Gestión proactiva del riesgo.
- Automatización de controles de seguridad donde sea posible.
- Cumplimiento con normativas como ISO/IEC 27001, NIST, GDPR y leyes locales.

4. Políticas Clave

4.1. Gestión de Identidades y Accesos

- Autenticación multifactor (MFA) obligatoria.
- Acceso basado en roles (RBAC).
- Revisión trimestral de permisos en sistemas críticos (repositorios de código, bases de datos, entornos de producción).

Política de Ciberseguridad Corporativa

4.2. Desarrollo Seguro (DevSecOps)

- Escaneo de código automatizado para vulnerabilidades (SAST/DAST).
- Evaluación de librerías de terceros y dependencias (Software Composition Analysis).
- Restricción de secretos/API keys en repositorios.

4.3. Protección de Infraestructura y Redes

- Segmentación de red.
- Monitorización continua y SIEM activo.
- Políticas de Zero Trust para entornos distribuidos y trabajo remoto.

4.4. Seguridad en la Nube

- Accesos cifrados y auditados a recursos en la nube (AWS, Azure, GCP).
- Uso de cuentas separadas por entorno (dev/staging/prod).
- Backups automáticos y verificación periódica de restauración.

4.5. Gestión de Dispositivos

- Equipos de trabajo deben tener EDR activo.
- Acceso remoto solo a través de VPN corporativa.
- BYOD permitido bajo políticas estrictas de control y seguridad MDM.

Política de Ciberseguridad Corporativa

4.6. Concienciación y Cultura de Seguridad

- Formación continua en ingeniería segura y ciberhigiene.
- Simulacros de phishing trimestrales.
- Cultura de “verificar siempre”, no “confiar por defecto”.

4.7. Gestión de Incidentes

- Canal directo y confidencial para reporte de incidentes (por ejemplo, en Slack o por email).
- Manual de respuesta a incidentes por tipo (data leak, ransomware, DDoS, etc.).
- Lecciones aprendidas y mejoras continuas post-incidente.

5. Cumplimiento y Auditoría

- Auditorías semestrales.
- Revisión externa anual de controles de seguridad.
- Política de sanciones según el nivel de incumplimiento.

6. Actualización de la Normativa

- Revisión anual o cuando haya cambios importantes en tecnologías o normativas.
- Publicación de versiones con cambios destacados para los equipos.